



#4
Pronto
Papier
HPP
4/15/02

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **30 AVR. 2001**

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE


THIS PAGE BLANK (USF 2)

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 260899

REMISE DES PIÈCES DATE 18 AVRIL 2000 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0004990 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 18 AVR. 2000		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE <p style="text-align: center;">Cabinet Philippe PRUGNEAU • Bernard SCHAUB 36, rue des Petits Champs 75002 PARIS Tél.: 01 40 20 16 16 - Fax: 01 40 20 90 07</p>	
Vos références pour ce dossier (facultatif) BR-25519/FR			
C nfirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie			
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i> <i>ou demande de certificat d'utilité initiale</i>		N°	Date <input type="text"/> / <input type="text"/> / <input type="text"/>
		N°	Date <input type="text"/> / <input type="text"/> / <input type="text"/>
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/>	N° <input type="text"/> / <input type="text"/> / <input type="text"/>
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Procédé de sécurisation d'une communication pour un système d'accès dit "mains libres"			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date <input type="text"/> / <input type="text"/> / <input type="text"/> N° <input type="text"/> Pays ou organisation Date <input type="text"/> / <input type="text"/> / <input type="text"/> N° <input type="text"/> Pays ou organisation Date <input type="text"/> / <input type="text"/> / <input type="text"/> N° <input type="text"/> <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		VALEO ELECTRONIQUE	
Prénoms			
Forme juridique		Société Anonyme	
N° SIREN		6 . 0 . 6 . 0 . 2 . 0 . 0 . 7 . 1	
Code APE-NAF		3 . 4 . 3 . 2	
Adresse	Rue	2, avenue Fernand Pouillon Europarc	
	Code postal et ville	94042	CRETEIL
Pays		FRANCE	
Nationalité		Française	
N° de téléphone (facultatif)			
N° de télécopie (facultatif)			
Adresse électronique (facultatif)			

REMISE DES PIÈCES DATE 18 AVRIL 2000 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0004990 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	
Vos références pour ce dossier : <i>(facultatif)</i>		BR-25519/FR	
6 MANDATAIRE			
Nom		PRUGNEAU	
Prénom		Philippe	
Cabinet ou Société		CABINET PRUGNEAU-SCHAUB	
N° de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue	36 rue des Petits Champs	
	Code postal et ville	75002	PARIS
N° de téléphone <i>(facultatif)</i>		01 40 20 16 16	
N° de télécopie <i>(facultatif)</i>		01 40 20 90 07	
Adresse électronique <i>(facultatif)</i>			
7 INVENTEUR (S)			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		Paiement en deux versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention <i>(joindre un avis de non-imposition)</i> <input type="checkbox"/> Requête antérieurement à ce dépôt <i>(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :</i>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Philippe PRUGNEAU CPI N°960705		VISA DE LA PRÉFECTURE OU DE L'INPI 	

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° .1. / .1.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		BR-25519/FR	
N° D'ENREGISTREMENT NATIONAL		0004590	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
Procédé de sécurisation d'une communication pour un système d'accès dit "mains libres"			
LE(S) DEMANDEUR(S) :			
VALEO ELECTRONIQUE			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		GASCHER	
Prénoms		Alain	
Adresse	Rue	10 rue du Dahomey	
	Code postal et ville	75011	PARIS
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Le 18 avril 2000 Philippe PRUGNEAU CPI N°960705	

THIS PAGE BLANK (SEPTO)

L'invention porte sur un procédé de sécurisation d'une communication entre un dispositif de reconnaissance et un organe d'identification apte à communiquer avec le dispositif de reconnaissance de manière à ce que le
5 dispositif de reconnaissance puisse authentifier l'organe d'identification pour commander le déverrouillage d'ouvrants d'un véhicule et/ou autoriser le démarrage d'un véhicule, dans lequel l'authentification est basée sur une évaluation par le dispositif de reconnaissance d'un temps de réaction correspondant au temps qui s'écoule entre l'émission par le dispositif de
10 reconnaissance d'un premier signal en direction de l'organe d'identification et la réception par le dispositif de reconnaissance d'un second signal émis par l'organe d'identification en réponse au premier signal.

Un tel dispositif de reconnaissance avec un organe d'identification constitue un système d'accès dit « mains libres ». Avec un tel système
15 d'accès, l'utilisateur peut déverrouiller les ouvrants de son véhicule sans avoir à manipuler de clé ni de télécommande : le simple fait d'être porteur d'un organe d'identification, qui peut être un badge, lui permet de voir son véhicule se déverrouiller lorsque par exemple il actionne la poignée de la portière conducteur. Ce dispositif de reconnaissance peut encore autoriser le
20 démarrage du véhicule lorsqu'il a authentifié l'organe d'identification.

Dans un tel système, la communication bidirectionnelle sous forme d'échange de données entre le dispositif de reconnaissance et l'organe d'identification a généralement pour but que le dispositif de reconnaissance authentifie l'organe d'identification d'une part en vérifiant sa signature et
25 d'autre part en évaluant un temps de réaction dans l'échange de données. L'évaluation d'un temps de réaction a pour objectif de détecter un piratage par répéteur : si un premier pirate, muni d'un premier relais émetteur-récepteur, situé à proximité du véhicule, est en relation avec un second pirate, muni d'un second relais émetteur-récepteur situé à proximité du
30 porteur de l'organe d'identification, les deux pirates sont en mesure de déclencher un échange de données entre le dispositif de reconnaissance et l'organe d'identification, à l'insu du porteur de l'organe d'identification. Cela étant, le répéteur ainsi constitué augmente nécessairement le temps de réaction dans l'échange de données entre le dispositif de reconnaissance et
35 l'organe d'identification. En évaluant un temps de réaction, le dispositif de

reconnaissance peut donc détecter un piratage par répéteur, et par-là même, ne pas commander le déverrouillage des ouvrants du véhicule.

Pour qu'un tel système ait un degré de sécurité satisfaisant, il faut entre autres qu'il soit capable d'évaluer avec suffisamment de précision un tel temps
5 de réaction dans l'échange de données.

Typiquement, le dispositif de reconnaissance évalue le temps de réaction de l'échange de données en se basant sur une seule mesure : par exemple, il émet un premier signal, et l'organe d'identification répond par l'envoi d'un second signal, et le temps de réaction évalué par le dispositif de
10 reconnaissance pour l'ensemble de l'échange de données est l'intervalle de temps qui s'est écoulé entre l'émission du premier signal et la réception du second signal. Malheureusement, ce temps de réaction peut varier largement du fait des retards aléatoires introduits notamment par les différents composants électroniques (amplification, remise en forme d'un
15 signal reçu et autres) que comprennent le dispositif de reconnaissance et l'organe d'identification. Par conséquent, il est pratiquement impossible de discriminer le retard introduit par les composants du système d'un retard introduit par un répéteur pirate.

Le but de l'invention est de remédier à ces inconvénients.

20 A cet effet, l'invention a pour objet un procédé de sécurisation d'une communication entre un dispositif de reconnaissance et un organe d'identification apte à communiquer avec le dispositif de reconnaissance de manière à ce que le dispositif de reconnaissance puisse authentifier l'organe d'identification pour commander le déverrouillage d'ouvrants d'un véhicule
25 et/ou autoriser le démarrage d'un véhicule, dans lequel l'authentification est basée sur une évaluation par le dispositif de reconnaissance d'un temps de réaction correspondant au temps qui s'écoule entre l'émission par le dispositif de reconnaissance d'un premier signal en direction de l'organe d'identification et la réception par le dispositif de reconnaissance d'un
30 second signal émis par l'organe d'identification en réponse au premier signal, caractérisé en ce que dans le dispositif de reconnaissance, on mesure successivement plusieurs temps de réaction entre des émissions de premiers signaux et des réceptions de seconds signaux correspondants, en ce que l'on calcule une moyenne de ces temps de réaction et en ce que l'on
35 compare celle-ci à un seuil prédéterminé pour authentifier l'organe d'identification.

Avec ce procédé, on s'affranchit de la dispersion qui existe dans les temps de réaction mesurés. En effectuant une évaluation du temps de réaction par moyennage, par exemple de cent mesures successives effectuées au cours d'un même échange de données, on obtient une

5 moyenne de temps de réaction qui est stable pour des conditions normales (sans interposition d'un répéteur pirate). Alors que si l'on effectue cette évaluation sur la transmission d'un seul premier signal et d'un seul second signal, on obtient des résultats qui varient trop pour pouvoir détecter un répéteur pirate.

- 10 Selon un mode de mise en œuvre particulier du procédé selon l'invention, dans lequel les temps de réaction pris en compte dans le calcul de la moyenne sont les n plus petits temps de réaction mesurés, n valant le produit du nombre de temps de réaction mesurés par un pourcentage prédéfini, arrondi à l'entier supérieur, les temps de réaction les plus élevés
- 15 ne sont pas pris en compte dans la moyenne pour que l'évaluation du temps de réaction soit plus pertinente.

- Selon un autre mode de mise en œuvre particulier du procédé selon l'invention, dans lequel le dispositif de reconnaissance émet lesdits premiers signaux de telle façon que deux premiers signaux successifs sont séparés
- 20 par un intervalle de temps d'une durée aléatoire, il est impossible à un système de piratage de prévoir à quels instants il doit émettre les seconds signaux.

Un exemple de réalisation du procédé est décrit plus en détail ci-après et illustré sur le dessin annexé.

- 25 La figure 1 est une vue schématique d'un système d'accès mains libres avec un dispositif de reconnaissance et un organe d'identification.

La figure 2 est une représentation graphique d'un exemple d'échange de données entre le dispositif de reconnaissance et l'organe d'identification du système d'accès montré sur la figure 2.

- 30 La figure 3 est un algorithme illustrant le procédé selon l'invention

- La figure 1 montre de façon schématique un dispositif de reconnaissance 1 et un organe d'identification 2 d'un système d'accès dit « mains libres ». Dans cette figure, on voit un dispositif de reconnaissance 1 qui émet vers un organe d'identification 2 un signal magnétique via une antenne d'émission
- 35 sous la forme d'une bobine 3. Ce signal magnétique est récupéré par l'organe d'identification via une antenne de réception sous la forme d'une

bobine 4. Ce signal est remis en forme par un récepteur 5 de l'organe 2 qui le transmet à un microcontrôleur 6 qui peut émettre en réponse un autre signal vers le dispositif de reconnaissance au moyen d'un émetteur 7, ce signal étant reçu par le dispositif de reconnaissance au niveau d'un circuit 5 récepteur 8.

Plus particulièrement, le dispositif de reconnaissance 1 comprend un microcontrôleur 9 qui génère sous forme électrique le signal à émettre, lequel est amplifié par un amplificateur de puissance 10 avant d'être transmis à la bobine émettrice 3 qui convertit ce signal électrique en un 10 signal magnétique. Enfin, et afin de lui permettre d'interpréter les signaux émis par l'organe d'identification et de mesurer des temps de réaction, le microcontrôleur 9 est aussi connecté au circuit récepteur 8 du dispositif de reconnaissance.

Dans ce système d'accès, la communication entre le dispositif de 15 reconnaissance 1 et l'organe d'identification 2 peut par exemple être déclenchée par l'actionnement d'une poignée d'un ouvrant du véhicule.

Pour ce qui concerne l'échange de données en lui-même, un exemple particulier est décrit ci-dessous. Il est important de noter que cet exemple est donné afin de faciliter la compréhension du procédé selon l'invention et qu'il 20 n'est en rien limitatif.

Dans cet exemple d'échange de données, les signaux échangés sont des impulsions, et le principe de l'échange consiste à ce que le dispositif de reconnaissance émette en direction de l'organe d'identification une première suite de bits, à laquelle l'organe d'identification doit répondre par une autre 25 suite de bits qu'il a calculée à partir de la suite de bits reçue de la part du dispositif de reconnaissance. Dans cet exemple, la transmission de la suite de bits correspondant à la réponse de l'organe d'identification est cadencée par des tops, qui sont des impulsions, émis par le dispositif de reconnaissance. Plus particulièrement, l'organe d'identification communique 30 le n-ième bit réponse après réception du n-ième top émis par le dispositif de reconnaissance, et le dispositif de reconnaissance interprète que ce bit vaut 1 s'il reçoit une impulsion dans un temps suffisamment court et qu'il vaut 0 sinon.

Dans l'échange de données qui est pris pour exemple figure 2, l'organe 35 d'identification a calculé qu'il doit fournir en réponse la suite de bits 1011 : après avoir perçu le premier top A émis par le dispositif de reconnaissance, il

va émettre par exemple une impulsion I1 (correspondant à « 1 ») ; après le second top B, il ne va rien émettre (ce qui correspond à « 0 ») ; après le troisième top C, il va émettre une impulsion I3; et après le quatrième top D, il va émettre une impulsion I4. De cette façon, le dispositif de reconnaissance

5 sait que la réponse de l'organe d'identification est 1011, et connaît trois temps de réaction dA, dC et dD, dont il va faire la moyenne. Dans un tel procédé, plus le nombre de bits réponse est élevé, plus l'évaluation du temps de réaction est précise, si bien qu'on aura intérêt par exemple à appliquer un protocole d'échange de données dans lequel la réponse fournie

10 par l'organe d'identification comportera par exemple cent bits réponse. Pour des raisons évidentes, le temps de réaction dans des conditions normales est nettement inférieur à l'intervalle de temps qui sépare deux tops successifs émis par le dispositif de reconnaissance.

La figure 3 donne de façon schématique un algorithme représentatif du

15 procédé selon l'invention : au cours d'une première étape 30, le dispositif de reconnaissance effectue une série de mesures de temps de réaction dt entre des signaux émis E et des signaux reçus R, et stocke ces temps de réaction dans un registre. Après que cette première étape ait été terminée, le dispositif de reconnaissance calcule en 31 la moyenne m de ces temps de

20 réaction, avant d'effectuer en 32 une comparaison entre la moyenne obtenue et une valeur de référence Ref prédéterminée, pour conclure selon le résultat que fournit cette comparaison s'il doit ou non autoriser le déverrouillage du véhicule.

D'autre part, le calcul de la moyenne des temps de réaction mesurés par

25 le dispositif de reconnaissance peut être affiné comme suit : pour cent temps de réaction mesurés dans un même échange, on pourra par exemple ne prendre en compte dans la moyenne que les quatre-vingt-dix bits temps de réaction les plus petits, de manière à écarter les temps de réaction abhérants. Plus particulièrement, dans ce mode de calcul, on se donne un

30 pourcentage prédéfini (ici 90%) de temps de réaction mesurés qui seront pris en compte. En effet, le nombre de mesures de temps de réaction effectuées au cours d'un échange de données peut ne pas être complètement prédéfini, comme le montre l'exemple illustré par la figure 2, dans lequel la transmission de quatre bits de données ne donne lieu qu'à

35 trois mesures de temps de réaction, et par suite, il est judicieux de prédéfinir un pourcentage de temps mesurés qui seront pris en compte, qui est



multiplié par le nombre de temps mesurés, et donne le nombre n de temps mesurés à prendre en compte.

Comme on le voit, on a un procédé pour lequel on peut d'une part affiner la résolution en augmentant le nombre de bits transmis, et d'autre part
5 adapter la tolérance en jouant sur le type de moyennage que l'on applique aux temps de réaction qui sont mesurés par le dispositif de reconnaissance.

En variante, les tops successifs A,B,C,D sont émis successivement par le dispositif de reconnaissance avec un intervalle de temps séparant deux tops consécutifs d'une durée aléatoire, par exemple par l'intermédiaire d'un jitter,
10 pour rendre plus difficile la substitution de l'organe d'identification par un dispositif pirate.

REVENDICATIONS

1/ Un procédé de sécurisation d'une communication entre un dispositif de reconnaissance (1) et un organe d'identification (2) apte à communiquer avec le dispositif de reconnaissance de manière à ce que le dispositif de reconnaissance puisse authentifier l'organe d'identification pour commander le déverrouillage d'ouvrants d'un véhicule et/ou autoriser le démarrage d'un véhicule, dans lequel l'authentification est basée sur une évaluation par le dispositif de reconnaissance d'un temps de réaction correspondant au temps qui s'écoule entre l'émission par le dispositif de reconnaissance d'un premier signal en direction de l'organe d'identification et la réception par le dispositif de reconnaissance d'un second signal émis par l'organe d'identification en réponse au premier signal, caractérisé en ce que dans le dispositif de reconnaissance, on mesure (30) successivement plusieurs temps de réaction (dA,dC,dD) entre des émissions de premiers signaux (A,B,C,D) et des réceptions de seconds signaux correspondants (I1,I3,I4), en ce que l'on calcule une moyenne de ces temps de réaction (31) et en ce que l'on compare celle-ci (32) à un seuil prédéterminé pour authentifier l'organe d'identification.

20

2/ Le procédé selon la revendication 1, dans lequel les temps de réaction pris en compte dans le calcul de la moyenne sont les n plus petits temps de réaction mesurés, n valant le produit du nombre de temps de réaction mesurés par un pourcentage prédéfini, arrondi à l'entier supérieur.

25

3/ Le procédé selon la revendication 1 ou 2, dans lequel le dispositif de reconnaissance émet lesdits premiers signaux de telle façon que deux premiers signaux successifs sont séparés par un intervalle de temps d'une durée aléatoire.

30

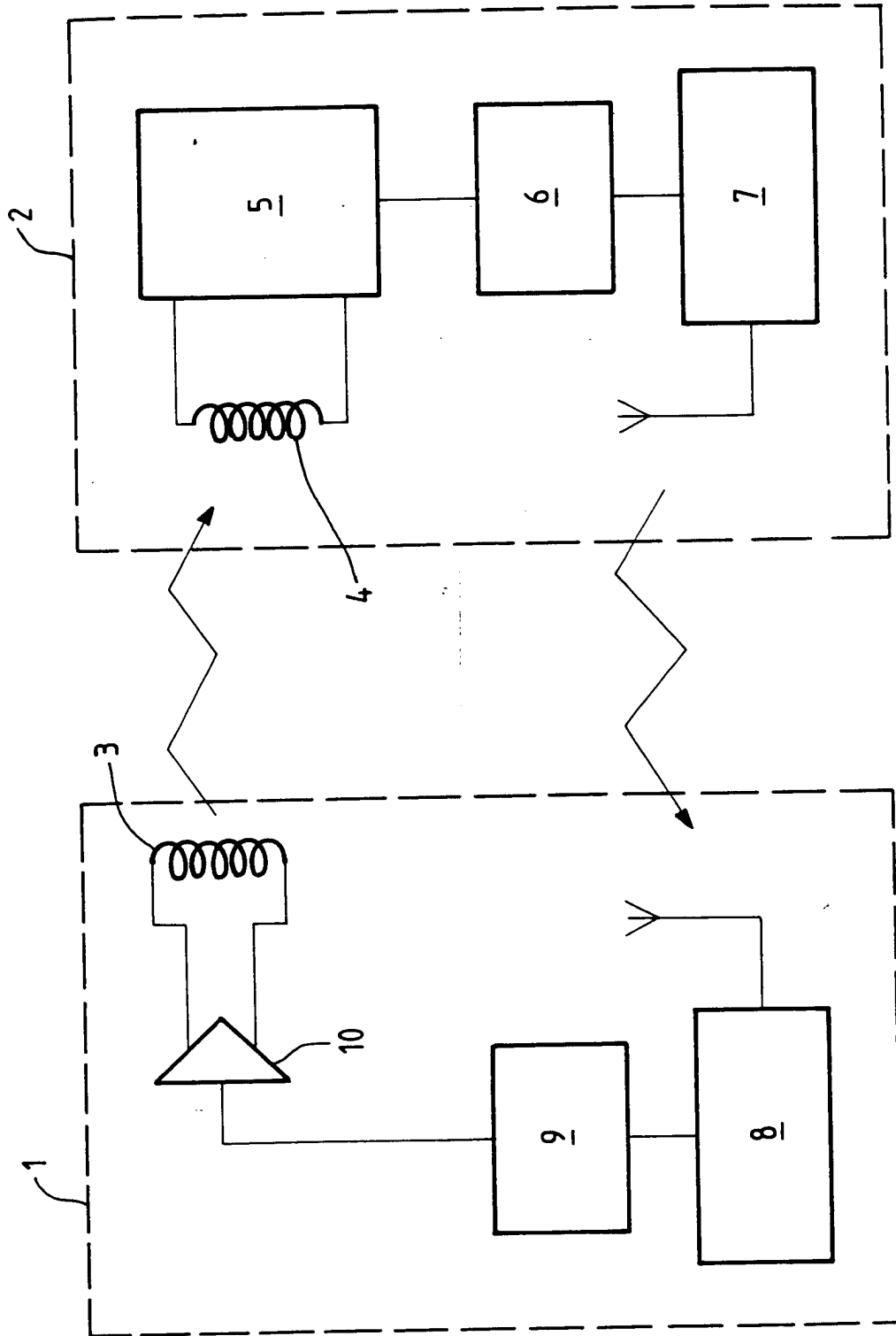
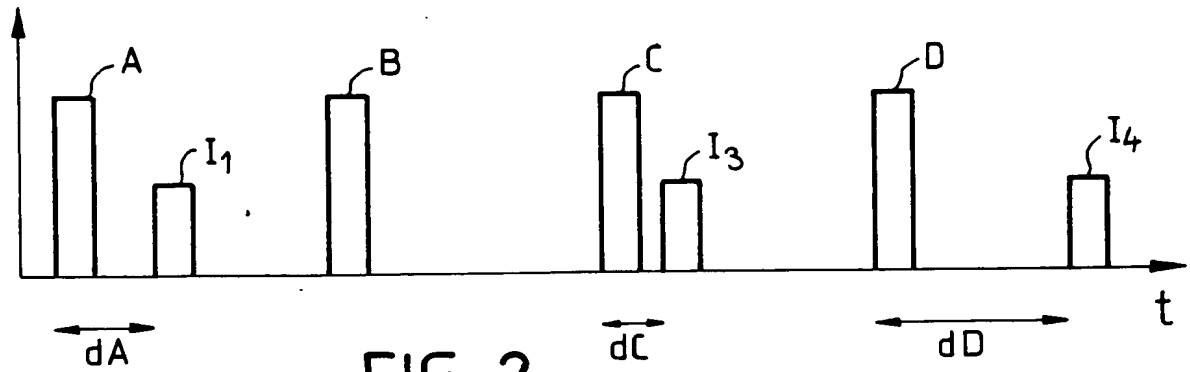
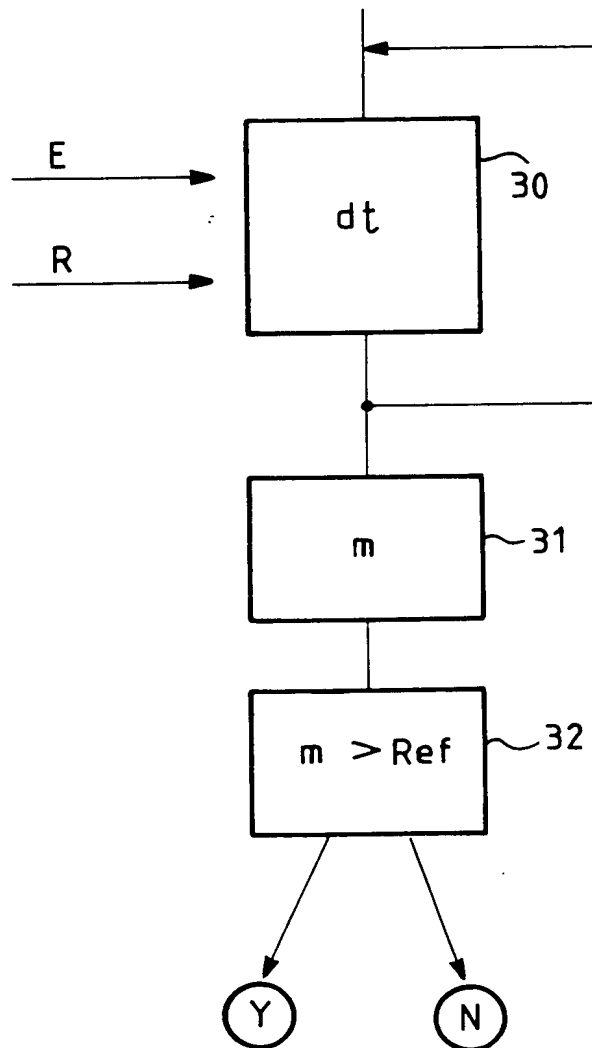


FIG-1

2/2



FIG_2



FIG_3

REVENDICATIONS

- 1/ Un procédé de sécurisation d'une communication entre un dispositif de reconnaissance (1) et un organe d'identification (2) apte à communiquer
5 avec le dispositif de reconnaissance de manière à ce que le dispositif de reconnaissance puisse authentifier l'organe d'identification pour commander le déverrouillage d'ouvrants d'un véhicule et/ou autoriser le démarrage d'un véhicule, dans lequel l'authentification est basée sur une évaluation par le
10 dispositif de reconnaissance d'un temps de réaction correspondant au temps qui s'écoule entre l'émission par le dispositif de reconnaissance d'un premier signal en direction de l'organe d'identification et la réception par le dispositif de reconnaissance d'un second signal émis par l'organe d'identification en réponse au premier signal, caractérisé en ce que dans le dispositif de reconnaissance, on mesure (30) successivement plusieurs temps de
15 réaction (dA,dC,dD) entre des émissions de premiers signaux (A,B,C,D) et des réceptions de seconds signaux correspondants (I1,I3,I4), et l'on calcule une moyenne de ces temps de réaction (31) que l'on compare (32) à un seuil prédéterminé pour authentifier l'organe d'identification, et en ce que le
20 dispositif de reconnaissance émet lesdits premiers signaux de telle façon que deux premiers signaux successifs sont séparés par un intervalle de temps d'une durée aléatoire.

- 2/ Le procédé selon la revendication 1, dans lequel les temps de réaction pris en compte dans le calcul de la moyenne sont les n plus petits temps de
25 réaction mesurés, n valant le produit du nombre de temps de réaction mesurés par un pourcentage prédéfini, arrondi à l'entier supérieur.